

CSfC Selections for TLS Protected Servers

TLS Protected Server products used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP's Protection Profile for Network Devices (NDPP) and this validated compliance shall include the selectable requirements contained in this document.

CSfC selections for NDPP evaluations:

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*